In The Claims:

1-22. (Canceled).

23. (Previously presented) A computer program product for providing a secure, integrated device with dynamically selectable capabilities, the computer program product embodied on one or more computer-usable media and comprising:

computer-readable program code that is configured to operate a security core which provides security functions;

computer-readable program code that is configured to establish a secure, operable connection of one or more components to the security core, such that the security core can vouch for authenticity of each securely operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device; and

computer-readable program code that is configured to securely perform a transaction using the secure integrated device, wherein the computer-readable program code that is configured to securely perform a transaction further comprises computer-readable program code that is configured to digitally notarize, by the security core, an output data stream created by a selected one of the operably connected components of the secure integrated device, and wherein the computer-readable program code that is configured to digitally notarize further comprises:

computer-readable program code that is configured to authenticate the selected operably connected component to the security core;

computer-readable program code that is configured to compute, by the security core, a hash value over the output data stream;

computer-readable program code that is configured to hash, by the security core, a combination of (1) the hash value and (2) the unique identifier of the selected operably connected component, thereby creating a hashed data block;

computer-readable program code that is configured to digitally sign, by the security core, the hashed data block using a private key of the security core; and

computer-readable program code that is configured to provide the digitally signed hashed data block along with the combination as the digital notarization of the output data stream.

24. (Previously presented) The computer program product according to Claim 23, wherein the computer-readable program code that is configured to authenticate further comprises computer-readable program code that is configured to use a unique identifier of the selected operably connected component, where the unique identifier is digitally signed by the selected operably connected component using a first private key associated with the selected operably connected component.

25. (Previously presented) A computer program product for providing a secure, integrated device with dynamically selectable capabilities, the computer program product embodied on one or more computer-usable media and comprising:

computer-readable program code that is configured to operate a security core which provides security functions;

computer-readable program code that is configured to establish a secure, operable connection of one or more components to the security core, such that the security core can vouch for authenticity of each securely operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device; and

computer-readable program code that is configured to securely perform a transaction using the secure integrated device, wherein the computer-readable program code that is configured to securely perform a transaction further comprises computer-readable program code that is configured to digitally notarize, by the security core, an output data stream created by a selected one of the operably connected components of the secure integrated device, and wherein the computer-readable program code that is configured to digitally notarize further comprises:

computer-readable program code that is configured to authenticate the selected operably connected component to the security core;

computer-readable program code that is configured to compute, by the security core, a hash value over each of a plurality of segments of the output data stream, wherein a boundary between segments is determined by an elapsed time value;

computer-readable program code that is configured to hash, by the security core, a combination of (1) the hash value for each segment and (2) the unique identifier of the selected operably connected component, thereby creating a hashed data block for each segment;

computer-readable program code that is configured to digitally sign, by the security core, the hashed data block for each segment using a private key of the security core; and

computer-readable program code that is configured to provide the digitally signed hashed data block for each segment along with the combination for each segment as the digital notarization of the segments which comprise the output data stream.

26. (Previously presented) The computer program product according to Claim 25, wherein the computer-readable program code that is configured to authenticate further comprises computer-readable program code that is configured to use a unique identifier of the selected operably connected component, where the unique identifier is digitally signed by the selected operably connected component using a first private key associated with the selected operably connected component.

27. (Original) The computer program product according to Claim 25, wherein authenticity of selected ones of the digitally notarized segments of the output data stream may be separately verified using a public key of the security core.

28. (Previously presented) The computer program product according to Claim 23 or Claim 25, further comprising:

computer-readable program code that is configured to authenticate a user of the secure integrated device; and

computer-readable program code that is configured to include an identification of the authenticated user in the combination.

29. (Original) The computer program product according to Claim 23 or Claim 25, wherein the private key of the security core is securely stored in the secure integrated device.

30. (Previously presented) The computer program product according to Claim 23, further comprising computer-readable program code that is configured to verify authenticity of the output data stream by a receiver of the output data stream and the digitally signed hashed data block, using a public key of the security core, and to conclude that the output data stream is authentic if the verification succeeds.

31. (Previously presented) The computer program product according to Claim 30, wherein the computer-readable program code that is configured to verify authenticity further comprises computer-readable program code that is configured to obtain the public key from a digital certificate of the security core.

32. (Previously presented) The computer program product according to Claim 30, wherein the computer-readable program code that is configured to verify authenticity further comprises computer-readable program code that is configured to conclude that the output data stream has not been tampered with if the verification succeeds.

33-62. (Canceled).

63. (Previously presented) A system for providing a secure, integrated device with dynamically selectable capabilities, comprising:

a security core which provides security functions;

one or more components;

means for operating the security core;

means for establishing a secure, operable connection of the components to the security core, such that the security core can vouch for authenticity of each securely operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device; and

means for securely performing a transaction using the secure integrated device, wherein the means for securely performing a transaction further comprises means for digitally notarizing, by the security core, an output data stream created by a selected one of the operably connected components of the secure integrated device, and wherein the means for digitally notarizing further comprises:

means for authenticating the selected operably connected component to the security core;

means for computing, by the security core, a hash value over the output data stream;

means for hashing, by the security core, a combination of (1) the hash value and (2) the unique identifier of the selected operably connected component, thereby creating a hashed data block;

means for digitally signing, by the security core, the hashed data block using a private key of the security core; and

means for providing the digitally signed hashed data block along with the combination as the digital notarization of the output data stream.

64. (Original) The system according to Claim 63, wherein the means for authenticating further comprises means for using a unique identifier of the selected operably connected component, where the unique identifier is digitally signed by the selected operably connected component using a first private key associated with the selected operably connected component.

65. (Previously presented) A system for providing a secure, integrated device with dynamically selectable capabilities, comprising:

a security core which provides security functions;

one or more components;

means for operating the security core;

means for establishing a secure, operable connection of the components to the security core, such that the security core can vouch for authenticity of each securely operably connected

component, wherein the security core and the operably connected components thereby comprise the secure integrated device; and

means for securely performing a transaction using the secure integrated device, wherein the means for securely performing a transaction further comprises means for digitally notarizing, by the security core, an output data stream created by a selected one of the operably connected components of the secure integrated device, and wherein the means for digitally notarizing further comprises:

means for authenticating the selected operably connected component to the security core;

means for computing, by the security core, a hash value over each of a plurality of segments of the output data stream, wherein a boundary between segments is determined by an elapsed time value;

means for hashing, by the security core, a combination of (1) the hash value for each segment and (2) the unique identifier of the selected operably connected component, thereby creating a hashed data block for each segment;

means for digitally signing, by the security core, the hashed data block for each segment using a private key of the security core; and

means for providing the digitally signed hashed data block for each segment along with the combination for each segment as the digital notarization of the segments which comprise the output data stream.

66. (Original) The system according to Claim 65, wherein the means for authenticating further comprises means for using a unique identifier of the selected operably connected component, where the unique identifier is digitally signed by the selected operably connected component using a first private key associated with the selected operably connected component.

67. (Original) The system according to Claim 65, wherein authenticity of selected ones of the digitally notarized segments of the output data stream may be separately verified using a public key of the security core.

68. (Original) The system according to Claim 63, further comprising:

means for authenticating a user of the secure integrated device; and

means for including an identification of the authenticated user in the combination.

69. (Original) The system according to Claim 65, wherein the private key of the security core is securely stored in the secure integrated device.

70. (Original) The system according to Claim 65, further comprising means for verifying authenticity of the segments of the output data stream by a receiver of the segments of the output data stream and the digitally signed hashed data blocks for the segments, using a

public key of the security core, and for concluding that each segment of the output data stream is authentic if the verification succeeds.

71. (Original) The system according to Claim 70, wherein the means for verifying authenticity further comprises obtaining the public key from a digital certificate of the security core.

72. (Original) The system according to Claim 70, wherein the means for verifying authenticity further comprises concluding that the output data stream has not been tampered with if the verification succeeds.

73-102. (Canceled).

103. (Previously presented) A method of providing a secure, integrated device with dynamically selectable capabilities, comprising:

operating a security core which provides security functions;

establishing a secure, operable connection of one or more components to the security core, such that the security core can vouch for authenticity of each secure operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device; and

securely performing a transaction using the secure integrated device, wherein securely performing a transaction further comprises digitally notarizing, by the security core, an output data stream created by a selected one of the operably connected components of the secure integrated device, wherein digitally notarizing further comprises:

authenticating the selected operably connected component to the security core;

computing, by the security core, a hash value over the output data stream;

hashing, by the security core, a combination of (1) the hash value and (2) the unique identifier of the selected operably connected component, thereby creating a hashed data block;

digitally signing, by the security core, the hashed data block using a private key of the security core; and

providing the digitally signed hashed data block along with the combination as the digital notarization of the output data stream.

104. (Previously presented) The method according to Claim 103, wherein authenticating further comprises using a unique identifier of the selected operably connected component, where the unique identifier is digitally signed by the selected operably connected component using a first private key associated with the selected operably connected component.

105. (Previously presented) A method of providing a secure, integrated device with dynamically selectable capabilities, comprising:

operating a security core which provides security functions;

establishing a secure, operable connection of one or more components to the security core, such that the security core can vouch for authenticity of each secure operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device; and

securely performing a transaction using the secure integrated device, wherein securely performing a transaction further comprises digitally notarizing, by the security core, an output data stream created by a selected one of the operably connected components of the secure integrated device, wherein the digitally notarizing further comprises:

authenticating the selected operably connected component to the security core;

computing, by the security core, a hash value over each of a plurality of segments of the output data stream, wherein a boundary between segments is determined by an elapsed time value;

hashing, by the security core, a combination of (1) the hash value for each segment and (2) the unique identifier of the selected operably connected component, thereby creating a hashed data block for each segment;

digitally signing, by the security core, the hashed data block for each segment using a private key of the security core; and

providing the digitally signed hashed data block for each segment along with the combination for each segment as the digital notarization of the segments which comprise the output data stream.

106. (Previously presented) The method according to Claim 105, wherein the authenticating further comprises using a unique identifier of the selected operably connected component, where the unique identifier is digitally signed by the selected operably connected component using a first private key associated with the selected operably connected component.

107. (Original) The method according to Claim 105, wherein authenticity of selected ones of the digitally notarized segments of the output data stream may be separately verified using a public key of the security core.

108. (Previously presented) The method according to Claim 105, further comprising:

authenticating a user of the secure integrated device; and

including an identification of the authenticated user in the combination.

109. (Original) The method according to Claim 103, wherein the private key of the security core is securely stored in the secure integrated device.

110. (Previously presented) The method according to Claim 105, further comprising verifying authenticity of the segments of the output data stream by a receiver of the segments of the output data stream and the digitally signed hashed data blocks for the segments, using a public key of the security core, and concluding that each segment of the output data stream is authentic if the verification succeeds.

111. (Previously presented) The method according to Claim 110, wherein verifying authenticity further comprises obtaining the public key from a digital certificate of the security core.

112. (Previously presented) The method according to Claim 110, wherein verifying authenticity further comprises concluding that the output data stream has not been tampered with if the verification succeeds.

113-116. (Canceled).